

### **REMARKS/ARGUMENTS**

Claims 1-12 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,289,462 to McNabb in view of U.S. Pat. No. 6,052,788 to Wesinger. The Applicant takes issue with this characterization and requests reconsideration.

The Applicant submits that the references have been incorrectly applied against the claimed invention. McNabb does not teach the invention as substantially claimed, as asserted by the Examiner. The basic problem with McNabb is its (1) invalidation of "trust" in a trusted operating system at the outset (column 8 lines 54-61, column 10 lines 60-67, column 11 lines 3-5) by making significant modifications to the operating system (which the claimed invention specifically avoids), and (2) use of discretionary access control (DAC) in a context where mandatory access control (MAC) is both highly desirable and moreover requisite to establishing and maintaining the security and trusted aspects of information.

Specifically, the comparison of the upgrade/downgrade enforcer (UDE) of McNabb to the claimed Master Daemon (MD) is inappropriate, since in McNabb it involves creating an automated system that replaces mandatory access control by discretionary access control and creates obvious covert channels (in the case of the UDE) as compared to the Master Daemon in the claimed invention. By contrast, the claimed invention clearly states that the subordinate daemons, the subordinate processes, the subordinate threads, and the other defined actions are all constrained to operate within one of the configured domains at least as restrictive as the configured domain of the Master Daemon. This limitation points to the result, as it is taught in the specification, that the present invention implements and maintains the principle of strict dominance in *all* transactions and therefore strictly enforces mandatory access control with no need, desire, or requirement for any form of discretionary access control within the Master Daemon. Further, the Master Daemon of the claimed invention enforces strict dominance in access to all sources, be they datastreams (network packets and/or file access), processes, threads, users, or any other construct that can conceivably be mapped into a configured domain. Strict dominance under mandatory access control requires enforcement of "Write-Up (or equivalent) / Read-Down (or equivalent)"; the Master Daemon does not compromise on this

requirement. By contrast, the UDE of McNabb operates by changing the SL of inbound packets (Figures 1, 5, 6, and text column 11 lines 41-45, lines 60-61, column 13 lines 26-36, lines 55-60, column 14 lines 4-7). The Security Gate of McNabb is another feature not required by the present invention and which further illustrates the advantages of the present invention (column 14 lines 17-25 and elsewhere). This function is unnecessary in the present invention and is deemed to be detrimental to security by providing potential covert channels. Another key difference between the two inventions may be found in McNabb (column 16 lines 15-35), wherein McNabb makes it quite plain that SLs must be inspected not only by the UDE but also by the processes to which requests are forwarded (specifically, column 16 lines 31-32), whereas the purpose of the Master Daemon of the claimed invention is to eliminate the necessity of modifications to software under its control and limit security considerations to the Master Daemon alone, where they belong. Many more examples are evident and may be noted (most of column 16, parts of column 17).

In addition, since there are no modifications made to the file system or kernel nor to any other non-configuration portion of the underlying trusted operating system (specifically in the preferred embodiment of the invention), the inherent certified and validated trust level of that system is inviolate; therefore it does not require re-evaluation or re-certification as a trusted operating system after application/installation of a master daemon. (It is of course presumed that the trust level of the Master Daemon has been previously established through separate validation and certification completely independent of the underlying operating system upon which it will be eventually installed). For this reason alone, it is submitted that the claims of the present application, included the added claims, clearly distinguish over the art of record.

The combination with Wesinger does not cure the deficiencies of McNabb. Wesinger has been cited for teaching instantiating a process or thread. Such a teaching is also deficient, even if properly combined. McNabb is inherently flawed and so it can contain no suggestion of correction to achieve the present invention by reference to other teachings.

Appln. No. 09/588,801  
Amdt. dated July 22, 2004  
Reply to Office Action of January 29, 2004

PATENT  
Attorney Docket No. 020570-1.00US

**CONCLUSION**

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,



Kenneth R. Allen  
Reg. No. 27,301

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: (650) 326-2400  
Fax: (650) 326-2422  
KRA:deh  
60265768 v1